UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

CHAMBERS OF
MADELINE COX ARLEO
UNITED STATES DISTRICT JUDGE

MARTIN LUTHER KING COURTHOUSE
50 WALNUT ST. ROOM 4066
NEWARK, NJ 07101
973-297-4903

May 5, 2023

VIA ECF

LETTER ORDER

Re: IN RE: AMERICAN MEDICAL COLLECTION AGENCY, INC. CUSTOMER DATA SECURITY BREACH LITIGATION
Civil Action No. 19-md-2904

Dear Litigants:

Before the Court are Motions to Dismiss two Amended Consolidated Class Actions Complaints (the "FACs") [1] filed in connection with the instant multidistrict litigation ("MDL") by (1) Laboratory Corporation of America Holdings ("LabCorp"), ECF No. 347; and (2) Sonic Healthcare USA ("Sonic USA") and its alleged subsidiaries (the "Sonic Subsidiaries" and together with Sonic USA, "Sonic"), ECF No. 351. For the reasons set forth below, the Motions are **GRANTED IN PART** and **DENIED IN PART**.

I. BACKGROUND[2]

This MDL arises from a data breach suffered by Retrieval-Masters Creditors Bureau, Inc. d/b/a American Medical Collection Agency ("AMCA"). Defendants are primarily healthcare providers who hired AMCA as a collections vendor and provided AMCA with sensitive patient information to facilitate collections. Between late 2018 and March 2019, an unauthorized user or users gained access to an AMCA computer system containing the private information of millions of patients (the "Data Breach"). Plaintiffs are among those patients whose Personal Information was impacted by the Data Breach. Each FAC alleges claims against a different Defendant or group of Defendants.

On December 16, 2021, the Court granted in part and denied in part motions to dismiss the original consolidated class action complaints ("CCAC's"). See generally, 2021 Opinion. The Court identified three groups of plaintiffs: (1) patients who had allegedly suffered economic injuries resulting from the misuse of Personal Information (the "Group I Plaintiffs"); (2) patients who did not experience direct economic harm, but who alleged facts sufficient to infer that an

[1] This Letter Order addresses only the Motions to Dismiss the relevant FACs against (1) LabCorp, see ECF Nos. 318 ("LabCorp FAC"); and (2) Sonic, see ECF No. 321("Sonic FAC").

[2] As the Court has addressed the facts of this case in detail in its December 16, 2021 Opinion, ECF. No. 283 (the "2021 Opinion"), it summarizes only the facts necessary to address the present motions.

unauthorized user obtained the patient's Personal Information in the Data Breach (the Group II Plaintiffs"); and (3) patients who alleged that their Personal Information was stored in the compromised AMCA systems but do not allege any other facts to suggest that their information was actually accessed, downloaded, or misused by an unauthorized party (the "Group III Plaintiffs").[3] The Court dismissed for lack of standing (1) the claims of the Group III Plaintiffs because they did not allege an injury-in-fact and (2) the claims of one Group II Plaintiff, Sonic Plaintiff D. Davis, for lack of traceability. The Court held that the remaining Plaintiffs had sufficiently pled negligence, negligence per se[4] and certain state statutory violations,[5] but did not sufficiently plead unjust enrichment and breach of implied contract. Notably, the Court also dismissed the negligence claim of Sonic Plaintiff G. Anderson because she failed to plead that any specific Sonic entity owed her a duty of care. As a result, all the claims against Sonic were dismissed, while Group I and II LabCorp Plaintiffs' claims were permitted to proceed.

On March 31, 2022, Plaintiffs filed FACs against Sonic and LabCorp. Specifically, the FACs assert five common law claims: (1) negligence, (2) negligence per se, (3) breach of confidence, (4) invasion of privacy and (5) unjust enrichment. The LabCorp FAC also asserts violations of state consumer laws.[6] The instant Motions followed.

II. LEGAL STANDARD

1. Motion to Dismiss Under Rule 12(b)(1)

A motion to dismiss for lack of standing is properly brought pursuant to Rule 12(b)(1). See Bellentine v. United States, 486 F.3d 806, 810 (3d Cir. 2007). Under Rule 12(b)(1), a plaintiff bears the burden of persuading the Court that subject matter jurisdiction exists. See Kehr Packages, Inc. v. Fidelcor, Inc., 926 F.2d 1406, 1409 (3d Cir. 1991). In resolving a Rule 12(b)(1)

---

[3] Group III included two Sonic Plaintiffs: (i) Tim Collinsworth and (ii) Tonda Tate; and 15 LabCorp Plaintiffs: (i) Tracy Buhr, (ii) Susan Duckworth, (iii) Jennifer Haley, (iv) Justin Nelson-Carter, (v) David Finch, (vi) George Rothwell, (vii) Cassandra Jerry, (viii) Carol Kaplan, (ix) Brenda Evans, (x) Jesse Lebon, (xi) Wendy Wallach, (xii) Sheera Harris, (xiii) Isaac Williams-Winders, (xiv) Martha Cuviller, and (xv) Gina Allende.

[4] Specifically, the Court found that the negligence and negligence per se claims of the following Plaintiffs against LabCorp could proceed: Sherrie Palmer, Sandra Lassiter, Aleksander Nazemnikov, Tanya Harris, Holly Laufenberg, Tatyana Shulman, Kristopher Thomas, Rosaria Gadero, and Melanie Vazquez, Timothy Petri, Valerie Scott, Cameron Spencer, Lori Lamondie-Murphy, Debra Wrenn, Edith Thrower, Timothy Judelsohn, and Tiffany Goins.

[5] Specifically, the Court found that Tatyana Shulman's claim against LabCorp under the Massachusetts Consumer Protection Act could proceed.

[6] LabCorp Plaintiffs claim violations of: (i) California's Confidentiality of Medical Information Act, Cal. Civ. Code §56, et seq ("CMIA"); (ii) California Unfair Competition Law, Cal. Bus. & Prof. Code §§17200, et seq. ("UCL"); (iii) California's Consumers Legal Remedies Act, Cal. Civ. Code §§1750, et seq. ("CLRA"); (iv) Kansas's Protection of Consumer Information, Kan. Stat. Ann. §§50-7a02(a), et seq. ("KPCI"); (v) Kansas Consumer Protection Act, K.S.A. §§50-623, et seq. ("KSA"); (vi) Kentucky Computer Security Breach Notification Act, Ky. Rev. Stat. Ann. §§365.732, et seq. ("KCSBNA"); (vii) Kentucky Consumer Protection Act, Ky. Rev. Stat. §§367.110, et seq. ("KCPA"); (viii) Maryland Consumer Protection Act, Md. Code Ann. Com. Law §13-101, et seq. ("MCPA"); (ix) Maryland Person Information Protection Act, Md. Comm. Code §§14-3501, et seq.("MPIPA"); (x) Massachusetts Consumer Protection Act, Mass. Gen. Laws Ann. Ch. 93A, §§1, et seq. ("MACPA"); (xi) New York General Business Law, N.Y. Gen. Bus. Law §§349, et seq. ("NYGBL"); (xii) Pennsylvania Unfair Trade Practices and Consumer Protection Law, LAW, 73 Pa. Cons. Stat. §§201-2 & 201-3, et seq. ("PUTPCPL"); (xiii) Wisconsin's Notice of Unauthorized Acquisition of Person Information, Wis. Stat. §§134.98(2), et seq. ("WNUAPI"); and (xiv) Wisconsin Deceptive Trade Practices Act, Wis. Stat. §100.18 ("WDTPAA").

motion, a court first determines whether the motion presents a "facial" or "factual" attack. See Constitution Party of Pa. v. Aichele, 757 F.3d 347, 357 (3d Cir. 2014). A facial attack argues that a claim on its face "is insufficient to invoke the subject matter jurisdiction of the court," id. at 358, and "does not dispute the facts alleged in the complaint," Davis v. Wells Fargo, 824 F.3d 333, 346 (3d Cir. 2016). A court reviewing a facial attack must "consider the allegations of the complaint and documents referenced therein and attached thereto, in the light most favorable to the plaintiff." Constitution Party of Pa., 757 F.3d at 358. Here, Defendants' motions to dismiss for lack of standing present facial attacks because they challenge Plaintiffs' standing to bring this lawsuit according to the pleaded facts. The Court thus accepts as true the pleaded facts as they relate to Plaintiffs' standing and draws all reasonable inferences in Plaintiffs' favor. See Constitution Party of Pa., 757 F.3d at 358.

2. Motion to Dismiss Under Rule 12(b)(6)

In resolving a Rule 12(b)(6) motion to dismiss, the Court accepts all pleaded facts as true, construes the complaint in the plaintiff's favor, and determines "whether, under any reasonable reading of the complaint, the plaintiff may be entitled to relief." Phillips v. County of Allegheny, 515 F.3d 224, 233 (3d Cir. 2008) (internal quotation marks and citation omitted). To survive a motion to dismiss, the claims must be facially plausible, meaning that the pleaded facts "allow [] the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." Ashcroft v. Iqbal, 556 U.S. 662, 678 (2009). The allegations must be "more than labels and conclusions, and a formulaic recitation of the elements of a cause of action will not do." Bell Atl. Corp. v. Twombly, 550 U.S. 544, 555 (2007).

III. ANALYSIS

1. Standing

Defendants argue that the Court should dismiss Plaintiffs' claims because the FACs still fail to establish injury-in-fact for the Group III Plaintiffs, and traceability for Sonic Plaintiff D. Davis. The Court disagrees.

As discussed at length in the Court's 2021 Opinion, Plaintiffs must allege that their Personal Information was accessed, stolen, or misused to establish injury-in fact in the data breach context. LabCorp and Sonic Plaintiffs whom the Court previously placed in Group III have now alleged financial injury from identity theft, or misuse of their information though publication on the dark web or attempted identity theft. For example, LabCorp Plaintiff T. Buhr now alleges three attempts to open credit cards in her name, that her Experian account was hacked, the unauthorized use of her debit card, and an attempt to open a bank account in her name. LabCorp FAC ¶ 20. Further, every LabCorp and Sonic Plaintiff now alleges that his or her information has

been found on the Dark Web. See, e.g., LabCorp FAC ¶40.[7] Accordingly, every Plaintiff has sufficiently alleged injury-in-fact such that they are either in Group I[8] or Group II.[9]

Additionally, the Court's 2021 Opinion found that the allegation that Plaintiffs "would not have had their Personal Information compromised by hackers 'but for' Defendants' choice to contract with AMCA without maintaining any oversight," was sufficient to establish causation for Article III standing at this stage. 2021 Opinion at 21. The Court finds these allegations sufficient for every Plaintiff at issue here.[10] See [LabCorp FAC ¶ 227; Sonic FAC ¶ 284].

The Court therefore finds that former LabCorp and Sonic Group III Plaintiffs, now designated as part of either Group I or II, and Sonic Plaintiff D. Davis, have now sufficiently established standing to survive a motion to dismiss.

2. Failure to State a Claim[11]

In the Court's prior Opinion, it found that all but one Group I and II Plaintiffs had sufficiently plead negligence and negligence per se claims, but dismissed each breach of implied contract and unjust enrichment claim. The Court also dismissed all but one LabCorp claim for violation of a state consumer law. Here, the Court will address whether the FACs cured the deficiencies outlined in the Court's prior opinion and the sufficiency of the FACs regarding the claims of new Group I and II Plaintiffs.

A. Negligence Claims

The Defendants argue that (1) that Plaintiffs have not adequately pled the injury and damages elements of common law negligence; (2) Plaintiffs cannot premise their negligence per se claims on alleged violation of Section 5 of the FTC Act or HIPAA; and (3) Plaintiffs' negligence per se claims are not cognizable under the law of many Plaintiffs' home states. The Court disagrees regarding common law negligence, and again declines to dismiss negligence per se claims prior to discovery.

---

[7] The Court is not convinced by Defendants' arguments that some of allegations are insufficient for failure to further specify the information published on the dark web and when it was discovered. This level of specificity is not required at this stage, especially because the Court must accept the allegations as true and resolve inferences in favor of Plaintiffs. See Constitution Party of Pa., 757 F.3d at 357. The Defendants may renew their specificity and factual causation arguments after discovery.

[8] Group I now includes additional LabCorp Plaintiffs: (i) Justin Nelson-Carter (unauthorized charges); (ii) David Finch (unauthorized withdrawal and pre-paid debit card); (iii) Jesse Lebon (unauthorized charges); and (iv) Sheera Harris (fraudulent medical bill).

[9] Group II now include an additional Sonic Plaintiff: Tonda Tate (fraudulent credit account); and 7 LabCorp Plaintiffs: (i) Tracy Buhr (attempted charges and attempts to open credit and other accounts); (ii) Jennifer Haley (unauthorized credit inquiry); (iii) George Rothwell (increased phishing emails); (iv) Carol Kaplan (unauthorized credit inquiry); (vi) Wendy Wallach (information on dark web); (vii) Martha Cuviller (increased spam calls and email).

[10] The Court notes that Sonic Plaintiff D. Davis's alleged injury in April 2018 is still insufficient because the Sonic FAC fails to include any allegation supporting his contention that the data breach occurred prior to August 1, 2018. However, D. Davis's claims may proceed based on his separate allegation that his information was found on the dark web.

[11] The Court reiterates its decision that "it is premature to decide choice of law issues at this stage." 2021 Opinion at 25. "That said, the Court may still address several arguments raised by Defendants in the Motions regarding Plaintiffs' common law claims, where the potentially-applicable states' laws are not meaningfully distinct." Id. Furthermore, the parties again agree that the statutory claims should apply the law of each Plaintiff's respective state.

Defendants do not make any arguments regarding new Group I and II Plaintiffs that the Court did not address in its 2021 Opinion. Regarding the negligence claims, the Court found that Defendants owed Plaintiffs a duty to safeguard their Personal Information, and that Defendants breached that duty by failing to oversee AMCA's data security. 2021 Opinion at 27-28. The Court also found that Plaintiffs' allegations that their "Personal Information would not have been compromised but for" that breach were sufficient to establish causation, and that the injuries sufficient for standing were sufficient to allege damages at this stage. Id. at 29-30. The Court declined to address the negligence per se claims prior before the end of discovery and a choice of law decision. Id. at 32-33. Because the Defendants simply restate their previous negligence arguments, the Court again finds that the new Group I and II Plaintiffs have sufficiently alleged injury and damages such that their negligence and negligence per se claims may continue.[12]

The Court did dismiss Sonic Plaintiff Anderson's negligence claims for failure to "expressly allege the specific entities that collected, maintained, and failed to protect Anderson's Personal Information." Id. at 31. But now, each Sonic Plaintiff alleges the specific Sonic entity from which he or she received healthcare services and provided his or her Personal Information. See e.g., Sonic FAC. ¶¶ 17-19 (alleging that Anderson was a patient of CPL and Austin Pathology, and that those entities, along with Sonic and Aurora, sent her bills to AMCA for collections). The Sonic FAC also includes a detailed breakdown of the Sonic entities, and importantly alleges that "[a]lthough Sonic is the parent and management company of its subsidiaries, Sonic directly interacted with AMCA on behalf of its subsidiaries," providing "AMCA with the Personal Information of the patients of its subsidiaries CPL, AEL, CBLPath, and Sunrise." Id. ¶¶ 116-17, 125-28. The Sonic FAC includes similar allegations regarding Aurora and its subsidiaries. Id. ¶¶ 130-36. These allegations are sufficient to cure the group-pleading deficiencies identified in the Court's 2021 Opinion.[13]

B. Unjust Enrichment

The Defendants argue that Plaintiffs' unjust enrichment claim should be dismissed because Plaintiffs have not alleged how they profited from their Personal Information. The Court agrees.

In its 2021 Opinion, the Court found that Plaintiffs did not allege unjust enrichment because "beyond vague allegations that Defendants collected information for 'commercial gain,' [] the CCACs contain[ed] no facts showing how Defendants reaped monetary benefits or otherwise profited from Plaintiffs' Personal Information." 2021 Opinion at 33-34. The Court explained that unjust enrichment is appropriate in the data breach context when "businesses commoditize or receive an independent pecuniary benefit from holding the Personal Information," such as using the information for targeting advertising. Id. at 34 (citing In re Yahoo! Inc. Customer Security

[12] The Court notes that it has reserved its determination regarding the economic loss and other differing state damages doctrines for after discovery.

[13] The Sonic Defendants' argument that the Sonic FAC still does not sufficiently allege that Sonic or Aurora ever "collected, maintained, or transmitted" Plaintiffs' Personal information is incorrect. The Sonic FAC alleges that, as a matter of course, Sonic and Aurora stored and provided AMCA with the Personal information of their subsidiaries' patients and provided examples of such transmissions. See, e.g., Sonic FAC ¶¶ 117-120, 122-26, 132-33. While these allegations may not survive summary judgement—they are enough to plausibly allege that Sonic and Aurora had a duty to safeguard Plaintiffs' Personal Information.

Data Breach Lit., No. 16-2752, 2017 WL 3727318, at *14 (N.D. Cal. Aug. 30, 2017); In re Marriott, 440 F. Supp. 3d at 461).

Plaintiffs have not cured this deficiency. The FACs allege that the Personal Information is valuable to patients, and to criminals seeking to misuse that information. LabCorp FAC ¶¶ 160-73, 194-95; Sonic FAC ¶¶ 223-231, 251-52. However, the FACs do not explain how this information is independently valuable to the Defendants. Plaintiffs pay Defendants for medical services received and entrust their Personal Information incidental to those services. Allegations that Plaintiffs would not have engaged Defendants for medical services do not plausibly suggest that the Personal Information itself is a part of Defendants' business model. See Yingst v. Novartis AG, 63 F. Supp. 3d 412, 417 (D.N.J. 2014) (dismissing an unjust enrichment claim despite Plaintiff's argument that she unjustly paid the Defendant more for its product than other comparable products). The Court will therefore dismiss the unjust enrichment claims with prejudice, as further amendment would be futile.

C. Breach of Confidence

The Defendants argue that Plaintiffs' new breach of confidence claims should be dismissed because the FACs do not allege that Defendants affirmatively disclosed private information to the individuals who breached AMCA's systems.[14] The Court agrees.

Plaintiff's allegations are insufficient to plead breach on confidence under any state's law.[15] Breach of confidence requires "the unconsented, unprivileged disclosure to a third party of nonpublic information." Kamal v. J. Crew Grp., Inc., 918 F.3d 102, 114 (3d Cir. 2019). Plaintiffs must allege affirmative action on the part of the discloser. See, e.g., In re Brinker Data Incident Litig., 2020 WL 691848, at *22 (M.D. Fla. Jan. 27, 2020) (dismissing a breach of confidence claim where the plaintiffs failed to allege that the defendant did "any act that made [p]laintiffs' information known—the information was stolen by third-parties.")

Plaintiffs concede that they do not allege that Defendants affirmatively disclosed their information to the individuals who hacked AMCA. LabCorp Pl. Opp. at 13, ECF No. 362.[16] Instead, Plaintiffs rely on Defendants disclosure to AMCA. Id. However, the FACs do not plausibly allege that AMCA was an unauthorized third party. The Plaintiffs do not argue that they did not permit Defendants to share Personal Information with third party entities like AMCA for billing purposes. In fact, allegations that some Plaintiffs received collection notices from AMCA, or provided their information directly to AMCA, undermine the argument that AMCA was an unauthorized third party. See, e..g., LabCorp FAC ¶ 23; Sonic FAC ¶ 20. Furthermore, references

[14] The Court need not address the Defendants' other arguments for why the breach of confidence claims should be dismissed.

[15] Although the Court declined to conduct a full choice of law analysis at this time, Plaintiff's have not cited a case from any state supporting their argument that reckless disclosure to an authorized third party is sufficient to plead a breach of confidence claim. The only relevant case Plaintiffs cite involved the unauthorized disclosure of the plaintiff's attempted suicide by hospital staff to a professional regulatory body for investigation. Wildman v. Homa, 32 Pa. D. & C.4th 468, 472-73, 480 (Com. Pl. 1996) (granting defendant's summary judgement on a breach of confidence claim based on a lack of evidence that hospital staff acted with malice), aff'd, 698 A.2d 679 (Pa. Super. Ct. 1997). Those circumstances are entirely different from the Defendants' apparently authorized use of a third-party vendors for billing purposes here.

[16] Sonic Plaintiffs do not make any independent arguments on this point, and in other parts of their opposition, and instead "incorporate" the arguments of other sets of Plaintiffs. Sonic Pl. Opp. at 24, ECF No. 365. The Court notes that it has referred to those arguments of other Plaintiffs throughout this Order as requested.

to unauthorized disclosure in the breach of confidence claims clearly refer to the individuals who gained access through the data breach. LabCorp FAC ¶ 250 ("As a result of the Data Breach, there was an unauthorized disclosure of Plaintiffs' and Class Members' Personal Information"); Sonic FAC ¶310 (same). Plaintiffs' assertion that an "unauthorized disclosure occurred" because Defendants "failed to implement and maintain reasonable safeguards" sounds "in negligence not breach of confidence." In re Brinker, 2020 WL 691848, at *22. The Court declines Plaintiffs' apparent invitation to predict whether such a theory of breach of confidence law could exist where it has already permitted negligence claims to proceed.

D. Invasion of Privacy

Defendants argue that the new invasion of privacy claims should be dismissed because the Plaintiffs have not alleged intentional intrusion by the Defendants.[17] The Court agrees.

To plead invasion of privacy, Plaintiffs must plead that the Defendants "believe[d], or [was] substantially certain, that [they] lack[ed] the necessary legal or personal permission to commit the intrusive act." O'Donnell v. United States, 891 F.2d 1079, 1083 (3d Cir. 1989) (interpreting Pennsylvania law); In re Nickelodeon Consumer Priv. Litig., 827 F.3d 262, 293 (3d Cir. 2016) ("The New Jersey Supreme Court. . . has said that intrusion upon seclusion occurs whenever a plaintiff can show (i) an intentional intrusion (ii) upon the seclusion of another that is (iii) highly offensive to a reasonable person").[18] "[T]he intrusion, as well as the action, must be intentional." O'Donnell, 891 F.2d at 1083.

Plaintiffs argue that grossly negligent conduct, such as not conducting oversight of AMCA, is sufficient to support an invasion of privacy claim, but cite no authority supporting that argument. The cases Plaintiffs cite still required allegations suggesting intentional conduct by the Defendant regarding the intrusion. See, e.g., Savidge v. Pharm-Save, Inc., 2021 WL 3076786, at *4 (W.D. Ky. July 1, 2021) (finding allegations that the defendant (1) "was aware of the potential hazard for phishing schemes;" (2) "failed to provide training or establish policies and procedures for protecting personal and sensitive information of its employees;" and (3) "that one or more agents of [defendant] released the sensitive and personal information in the W-2s to third-party cybercriminals" sufficient to plausibly allege intentional conduct).

Here, Plaintiffs' allegations that Defendants neglected their duty to oversee AMCA are inadequate. See Kirsten 2022 WL 16894503 at *4 ("Plaintiffs have not provided anything specific regarding whether or how Defendant knew its security was deficient or any other allegations

[17] The Court need not address the Defendants' other arguments for why the invasion of privacy claims should be dismissed.

[18] See also Farmer v. Humana, Inc., 582 F. Supp. 3d 1176, 1188, at *18 (M.D. Fla. Jan. 25, 2022) ("invasion-of-privacy claim fails [under Florida Law] because [plaintiff] does not allege that [defendants] intentionally disclosed his [information] to unauthorized persons [but] that defendants' negligent failure to protect the [information] resulted in the disclosure"); Burton v. MAPCO Express, Inc., 47 F. Supp. 3d 1279, 1288 (N.D. Ala. 2014) (Under Alabama Law, "even if the defendants were negligent, as alleged, in safeguarding [plaintiff's] account information, such negligence does not morph into an intentional act of divulging his confidential information"); Mackey v. Belden, Inc., No. 4:21-CV-00149-JAR, 2021 WL 3363174, at *10 (E.D. Mo. Aug. 3, 2021) (Under Missouri Law, allegation that defendant "acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate" is inadequate to plead invasion of privacy); Kirsten v. California Pizza Kitchen, Inc., No. 221CV09578, 2022 WL 16894503, at *4 (C.D. Cal. July 29, 2022), reconsideration denied, No. 221CV09578, 2022 WL 16894880 (C.D. Cal. Sept. 8, 2022) ("The Ninth Circuit has held that to state a claim for invasion of privacy under California common law, "a plaintiff must plead that (1) a defendant 'intentionally intrude[d] into a place, conversation, or matter as to which the plaintiff has a reasonable expectation of privacy[,]' and (2) the intrusion 'occur[red] in a manner highly offensive to a reasonable person.'") (citation omitted).

indicating that Defendant intentionally allowed unauthorized access to Plaintiffs' [information]. Plaintiffs thus provide only conclusory allegations regarding intentional invasion of privacy in their FAC.") (citing In re Ambry, 567 F. Supp. 3d at 1143). The FACs come closer to alleging that AMCA acted knowingly by consciously disregarding the vulnerabilities in their systems; but even those allegations suggest that the vulnerabilities were not discovered until after the breach. See LabCorp FAC ¶¶ 94-97; Sonic FAC ¶¶ 158-74. Furthermore, AMCA is not a Defendant here. As discussed above, Section III.2.C, Plaintiffs have not alleged that Defendants disclosed their private information to hackers. Neither have Plaintiffs alleged facts suggesting that when Defendants shared information with AMCA, they did so with the intent to invade Plaintiff's privacy. Accordingly, the Court will dismiss the invasion of privacy claims.

E. Statutory Claims[19]

The LabCorp Defendants argue that Plaintiffs' have failed to state violations of their respective state's consumer and or data security statutes.[20] Specifically, the LabCorp Defendants argue that certain claims fail (1) for lack of Injury and Causation[21] or (2) because Plaintiffs have not alleged misrepresentations or omissions-based claims with particularity. LabCorp Defendants argue that the remaining statutory claims should be dismissed based on statute-specific rules. The Court will address each statute in turn, addressing statutes together only where the analysis is identical.

a) Omission-Based Claims

LabCorp first argues that Plaintiffs' omission-based statutory claims should be dismissed for failure to plead reliance with the particularity required. The Court agrees in part.

As discussed at length in the Court's 2021 Opinion, "Plaintiffs must satisfy Rule 9(b)['s heightened pleading standard] to the extent their statutory claims rely on alleged misrepresentations and knowing omissions made by Defendants." 2021 Opinion at 39-41. In

---

[19] The Court will not revisit its finding that LabCorp Plaintiff Tatyana Shulman has pled a MACPA claim based on unfair or deceptive practices. 2021 Opinion at 57-58.

[20] Plaintiffs state that they are no longer pursuing their Wisconsin and Pennsylvania consumer protection claims, or their Kentucky Data Breach notification claim LabCorp Pl. Opp. at 27 n.29, 37 n.33. Accordingly, those claims are dismissed.

[21] LabCorp makes broad arguments that Plaintiffs statutory claims fail for lack of injury and causation. However, as discussed above supra-Section III.1, each new Group I and Group II LabCorp Plaintiff has sufficiently alleged concrete injury and that the injury was caused by the data breach. Unless a statute specifically limits the type of injury, the Court will not dismiss the claim for lack of injury. In the 2021 Opinion, the Court found, with respect to the statues at issue here, the CLRA did not limit the type of injury required, while the UCL did.

Here, LabCorp's only specific challenge to LabCorp Plaintiff Kaplan's MCPA claim is that it should be dismissed because she does not allege and identifiable loss as the statute requires. The Court does not interpret the MCPA's requirement that a plaintiff plead "actual injury or harm" that is "objectively identifiable," Attias v. CareFirst, Inc., 365 F. Supp. 3d 1, 10 (D.D.C. 2019), on reconsideration in part, 518 F. Supp. 3d 43 (D.D.C. 2021) (citation omitted), as requiring only purely economic harms. Plaintiff Kaplan's allegations that she suffered an unauthorized credit inquiry after the data breach and that her Personal Information was found on the dark web, combined with the costs of mitigation, LabCorp FAC ¶ 27, are sufficient at this stage to plead actual injury. See In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig., 440 F. Supp. 3d 447, 494 (D. Md. 2020) ("Plaintiffs do not need to assign a value at [the motion to dismiss stage] stage to adequately plead damages").

The Court will address and apply each remaining statute's requirements in turn.

context of the facts of this case, Plaintiff must plead "that they read LabCorp's privacy policies before agreeing to blood testing" to establish reliance. Id. 55-56. See also, e.g, Tabler v. Panera LLC, 2020 WL 3544988, at *6-7 (N.D. Cal. Jun. 30, 2020) (dismissing UCL and CLRA claims for failure to allege specific facts regarding statements). In contrast, Plaintiffs' claims based on unlawfulness or unfairness may proceed if they plausibly allege the requirements of each statute. 2021 Opinion at 39-41.

Here, LabCorp Plaintiffs appear to assert omissions-based consumer protection claims under California's UCL and CLRA; Kansas's KSA; Kentucky's KCPA; Maryland's MCPA; Massachusetts's MACPA; and New York's NYGBL. Plaintiff Rothwell (Kentucky) did not allege that he read any privacy policy at all. See FAC ¶ 26. Similarly, Plaintiffs' Nazemnikov (California), Shulman (Massachusetts), Gadero (New York), and Wallach's (New York) allegations that each "does not recall" if he or she reviewed a privacy policy, or "believes" he or she did, id. ¶¶ 19, 28, 32, 33, are insufficient because omissions-based claims require particularity. The Court cannot find that these Plaintiffs relied on any omission by LabCorp if they are unsure whether they even read the policy at issue. Accordingly, these Plaintiffs' omissions-based consumer claims are dismissed.[22]

Other Plaintiffs have alleged that they read LabCorp's privacy policies at the time that they received services. Id. ¶¶ 18, 25, 27 (Lassiter-California; Finch-Kansas; and Kaplan-Maryland). These Plaintiffs have sufficiently alleged reliance, and therefore their omission-based statutory claims may proceed.

b) California CMIA

LabCorp argues that the CMIA claim should be dismissed because Plaintiffs failed to allege that LabCorp mishandled Plaintiff's medical information as defined by the statute. The Court disagrees.

The Court previously held that Plaintiffs failed to allege facts sufficient to show that their "medical information" was viewed or accessed by an unauthorized person as required under the CMIA. 2021 Opinion at 63-64 (explaining that CMIA covers information "regarding a patient's medical history, mental or physical condition, or treatment"); Cal. Civ. Code § 56.05. The LabCorp FAC now includes an explanation regarding LabCorp's transmission of patients' ICD codes, which "can be used to identify information relating to an individual's medical history, mental or physical condition, and treatment." LabCorp FAC ¶ 68. Plaintiffs allege that such ICD codes were stored on the AMCA's CHAMP database that was accessed as part of the data breach. Id. ¶¶ 86, 277.

LabCorp first argues that Plaintiffs did not specifically include ICD codes in their definition of Personal Information that was transmitted to AMCA. But the LabCorp FAC defines Personal Information broadly, including "information related to Plaintiffs' and Class Members' medical providers and services (such as dates of service and referring doctor)." Id. ¶ 6. The FAC plausibly suggests that when California Plaintiffs Lassiter and Nazemnikov alleged that LabCorp transmitted their Personal Information to AMCA, id. ¶¶ 18-19, that their ICD codes from which the specific medical diagnosis could be identified, were included. Defendant's fact arguments to the contrary are unavailing at the motion to dismiss stage.

LabCorp also argues that providing information to AMCA for billing purposes was expressly authorized by the CMIA, and that AMCA's subsequent actions or omissions cannot

[22] Because the NYGBL only permits misrepresentation or omission-based claims, LabCorp Plaintiffs Gadero and Wallach's claims are dismissed with prejudice, as further amendment would be futile.

create liability for LabCorp. LabCorp Br. at 22.[23] Plaintiffs concede that CMIA expressly authorizes health providers to disclose medical information to an "entity that provides billing, claims management, medical data processing, or other administrative services," Cal. Civ. Code § 56.10(c)(3), such as AMCA. However, Plaintiffs counter that the CMIA independently required LabCorp to take care to preserve the confidentiality of medical information when it "creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information." Cal. Civ. Code § 56.101(a). The Court agrees with Plaintiffs. LabCorp had a duty under the CMIA to safeguard medical information that included its oversight of AMCA. Plaintiffs have sufficiently alleged that LabCorp was negligent with respect to safeguarding their medical information. See supra-Section III.2.a.

Accordingly, the CMIA claims of LabCorp Plaintiffs Lassiter and Nazemnikov may proceed.

c) California's CLRA, Kansas's KSA, and Kentucky's KCPA

LabCorp argues that Plaintiffs' CLRA,[24] KSA, and KCPA[25] claims each fail because Plaintiffs do not allege that they purchased or leased any service or good, as each statute requires. Cal. Civ. Code §§ 1780(a), 1761(d); Kan. Stat. Ann. §§ 50-626(a), 50-624(c); Ky. Rev. Stat. Ann. § 367.220(1). The Court disagrees.

Plaintiffs' allegations that they were billed for LabCorp services are sufficient here.[26] LabCorp relies on cases dismissing these claims where the plaintiffs received free goods or

[23] The Defendants also argue that the CMIA requires only affirmative disclosure, and thus third-party hackers stealing the information from AMCA is not actionable. However, "[t]he plain text of the statute does not require an affirmative disclosure by the medical provider to create liability but in fact creates a remedy for those who store records negligently." In re Solara Med. Supplies, LLC Customer Data Sec. Breach Litig., 613 F. Supp. 3d 1284, 1299 (S.D. Cal. 2020) (citing Regents of Univ. of California v. Superior Ct., 163 Cal. Rptr. 3d 205, 217 (Cal. App. 4th 2013)).

[24] LabCorp also argues that the CLRA claim should be dismissed for lack sufficient of pre-suit notice. However, California state courts have clarified that federal courts requiring dismissal for lack of proper notice pursuant to the CLRA "fail to properly take into account the purpose of the notice requirement," which "exists in order to allow a defendant to avoid liability for damages if the defendant corrects the alleged wrongs within 30 days after notice, or indicates within that 30-day period that it will correct those wrongs within a reasonable time." Morgan v. AT&T Wireless Servs., Inc., 177 Cal. App. 4th 1235, 1261 (2009). Here, Plaintiffs provided notice immediately before their CCAC —over 2.5 years before the present FAC was filed. The Court will not dismiss the viable CLRA claim based on insufficient notice where the Defendant has been aware of the relevant allegations for far more than the 30 days required. See Whelan v. BDR Thermea, No. C-11-02146 EDL, 2011 WL 6182329, at *7 (N.D. Cal. Dec. 13, 2011) ("the issue of notice is moot now that Plaintiff has filed a second amended complaint after Defendant timely responded to the notice").

[25] Defendants' additional arguments regarding the statutory territorial requirement and prohibition against class actions are unavailing at this time. The parties are unable to cite any cases on regarding the purported territorial limit of the KCPA. And although the court is inclined to agree at least that the KCPA does not permit class actions in light of Arnold v. Microsoft Corp., 2000 WL 36114007, at *6 (Ky. Cir. Ct. July 21, 2000), *aff'd*, 2001 WL 1835377 (Ky. Ct. App. Nov. 21, 2001)—the parties disagree on over whether either prohibition is substantive such that 28 U.S.C. §1332 and Federal Rule 23 should not apply. The Court declines to dismiss the KCPA claims at this time given the limited briefing on the Erie dispute. See Chen v. Target Corp., 2022 WL 1597417, at *19 (D. Minn. May 19, 2022) (declining to dismiss class action claim under the KCPA because it was unclear whether the prohibition was substantive or procedural, and issue was insufficiently briefed). The Defendants may renew these arguments through supplemental briefing, or at summary judgment.

[26] The Court also notes that is not convinced that these statutes limit ascertainable loss such that the harms identified supra Section III.1 would be insufficient to establish damages. See Via Christi Reg'l Med. Ctr., Inc. v. Reed, 298 Kan. 503, 519, 314 P.3d 852, 864 (2013) ("a consumer need not establish measurable monetary damages to qualify as aggrieved" under the KSA); Complete Auto. Repair Servs. v. Capps, No. 2012-CA-002145-MR, 2015 WL 2445911,

services in exchange for their Personal Information. See Claridge v. RockYou, Inc., 785 F. Supp. 2d 855, 864 (N.D. Cal. 2011) (dismissing a CLRA claim based on plaintiff's "transfer of [Personal] [I]nformation to defendant in exchange for free applications"); Berry v. Nat'l Med. Servs., Inc., 205 P.3d 745, 752 (Kan. App. 2009), aff'd, 257 P.3d 287 (Kan. 2011) (dismissing a KSA claim where the plaintiff failed to allege facts suggesting that she "exchang[ed] anything of value with the defendants to secure their services). The facts here are wholly different. Plaintiffs allege that they used LabCorp's medical services and that their information was transmitted to AMCA for bill collections purposes. See LabCorp FAC ¶¶ 18, 26. These facts suggest that Plaintiffs received services in exchange for the promise to pay for those services. The Court is satisfied that LabCorp Plaintiffs Lassiter, Rothwell, and Finch have sufficiently alleged a purchase under the CLRA, KSA and KCPA.[27]

d) California's UCL

LabCorp argues that Plaintiffs' fraud and unlawfulness UCL claims should be dismissed because the Plaintiffs have not established that they lack an adequate remedy at law.[28] The Court agrees.

The UCL provides only equitable or injunctive relief for consumers harmed by a business's fraudulent, unlawful or unfair business practices. See Korea Supply Co. v. Lockheed Martin Corp., 63 P.3d 937, 943 (Cal. 2003). The Ninth Circuit has held that "the traditional principles governing equitable remedies in federal courts, including the requisite inadequacy of legal remedies, apply when a party requests restitution under the UCL and CLRA in a diversity action." Sonner v. Premier Nutrition Corp., 971 F.3d 834, 844 (9th Cir. 2020). LabCorp Plaintiffs Lassiter and Nazemnikov have alleged at least negligence and CMIA claims, and Lassiter has also alleged a CLRA claim for damages. Plaintiffs make no argument and have not otherwise "alleged any facts establishing that their remedies at law are inadequate." Watkins v. MGA Ent., Inc., 550 F. Supp. 3d 815, 838 (N.D. Cal. 2021).

Plaintiffs' allegations regarding future redressable harm "because LabCorp's oversight of its collection vendors may still be legally deficient and Plaintiffs' accounts may still be in collection, see LabCorp FAC ¶ 50, are still insufficient to justify injunctive relief. As the Court's 2021 Opinion explained, an injunction against LabCorp "will not prevent hackers already in possession of [Plaintiffs'] Personal Information from doing future harm." 2021 Opinion at 51. Furthermore, even accepting Plaintiffs' conclusory allegation that their accounts may still be in collections—Plaintiffs repeatedly allege that they "would not have used" LabCorp if they "had known it would not protect [their] Personal Information, rendering it 'unlikely that [they] will be deceived again.'" Id. (citing Johnson, 175 F. Supp. 3d at 1141).

---

at *5 (Ky. Ct. App. May 22, 2015), as modified (May 29, 2015) (concluding that "a person is not required to allege a specific amount of actual damages that he has already incurred as out-of-pocket expenses to make out a prima facie case under" the KCPA).

[27] As discussed above, supra-Section III.2.E.a, LabCorp Plaintiff Rothwell's omission based KSA claim must be dismissed. However, Rothwell's "unconscionable" practices based KSA claim may continue. Additionally, since California LabCorp Plaintiffs Lassiter and Nazemnikov assert only omissions based CLRA claims, only Lassiter's CLRA claim may continue.

[28] The Court need not reach LabCorp's other arguments for why the UCL claims should be dismissed.

The Court will therefore dismiss both LabCorp Plaintiffs Lassiter and Nazemnikov's UCL claims.[29]

e) Cybersecurity and Data Breach Statutes

LabCorp argues that the Cyber Security and Data Breach Notification claims brought pursuant to Kansas's KPCI, Wisconsin's WNUAPI, and Maryland's MPIPA should be dismissed because (1) the statutes do not have an enforceable private right of action and (2) LabCorp is exempt. The Court agrees in part.

LabCorp first argues that these claims must be dismissed because the statutes do not provide a private right of action. The Court agrees that neither the KPCI nor WNUAPI expressly provide a private cause of action. See Kan. Stat. Ann. § 50-7a02(g) ("the attorney general is empowered to bring an action in law or equity to address violations of this section" and "[t]he provisions of this section are not exclusive"); Wis. Stat. Ann. § 134.98(4) ("Failure to comply with this section is not negligence or a breach of any duty, but may be evidence of negligence or a breach of a legal duty"). Plaintiff counters with cases permitting these statutory claims to proceed past the motion to dismiss stage in the absence of authority precluding private rights of action. See In re Equifax, Inc., Customer Data Sec. Breach Litig., 362 F. Supp. 3d 1295, 1341 (N.D. Ga. 2019) ("The court [in Target] concluded that, absent any [contrary] authority, the plaintiffs' claim should survive. Likewise, the here concludes that, without any authority suggesting otherwise, this claim should survive.") (citing In re Target Corp. Customer Data Sec. Breach Litig., 66 F. Supp. 3d 1154, 1169-70 (D. Minn. 2014)). But here, LabCorp has cited contrary authority at least for the WNUAPI. Fox v. Iowa Health Sys., 399 F. Supp. 3d 780, 800 (W.D. Wis. 2019) ("Because the legislature has not provided any indication that § 134.98 creates a separate right of action, the court will dismiss plaintiffs' claims under the statute."). As a result, the Court will dismiss the WNUAPI claim.

Regarding MPIPA, although the statute does not provide an independent right of action, it provides that a violation is enforceable through the MCPA. Md. Code Ann. Com. Law § 14-3508. Therefore, the Court must dismiss the MPIPA claim to the extent that it stands apart from the MCPA claim, which the Court has already permitted to proceed.[30]

LabCorp next argues that the KCPI exempts entities regulated by HIPAA and that the MPIPA exempts entities that comply with HIPAA. The Court agrees but finds that only the KCPI claims require dismissal. With respect to the KCPI, the plain language of the statute exempts entities regulated by federal laws such as HIPAA. Kan. Stat. Ann. § 50-7a02(e) ("An [entity that is regulated by federal law] and that maintains procedures for a breach of the security of the system pursuant to the laws[] established by its primary or functional state or federal regulator is deemed to be in compliance with this section.").

---

[29] Any further amendment should detail the risk of future harm arising from LabCorp's conduct, other than the harm stemming from the past data breach.

[30] Specifically, the Court has permitted the omission based MCPA claim to proceed based on LabCorp Plaintiff Kaplan's reliance allegations. Any successfully alleged violations of MPIPA's data security requirements may proceed only as part of Kaplan's MCPA claim. As the Court has already found that the MCPA does not limit the type of damages recoverable, supra note 21, it is unnecessary to separately address this argument under the MPIPA. The parties factual dispute regarding the amount of damage flowing from the delayed notification vs. the data breach is better resolved after discovery.

With respect to the MPIPA,[31] however, the statute only exempts entities that comply with such regulations. Md. Code Ann. Com. Law § 14-3507(d)(1) ("A business that is subject to and in compliance with the federal Health Insurance Portability and Accountability Act of 1996 shall be deemed to be in compliance with this subtitle"). HIPAA requires notification of a data breach "without unreasonable delay and in no case later than 60 calendar days after discovery of a breach." 45 C.F.R. §164.404(b). The LabCorp FAC alleges the following: (1) LabCorp should have known of the Data Breach no later than March 2019 had LabCorp exercised reasonable diligence, LabCorp FAC ¶114; (2) LabCorp did not send any breach notice until June 4, 2019, id. ¶140; and (3) LabCorp did not post any information about the Data Breach on its website until July 13, 2019, id. ¶141. These allegations are sufficient to allege non-compliance with HIPAA's 60-day requirement at this stage.

Accordingly, the Court will dismiss the WNUAPI and KCPI claims, but permit the MPIPA claim to proceed as part of Plaintiff Kaplan's MCPA claim.

IV. CONCLUSION

For the reasons stated above, Defendants' Motions to Dismiss pursuant for lack of standing to Rule 12(b)(1), ECF Nos. 347, 351, are **DENIED.**

Defendants' Motions to Dismiss for failure to state a claim pursuant to Rule 12(b)(6), ECF Nos. 347, 351, are **GRANTED in part** and **DENIED in part.** The following claims may proceed:

1) The negligence and negligence per se claims of all Sonic and LabCorp Plaintiffs;
2) Sandra Lassiter and Aleksander Nazemnikov's claims against LabCorp under the California Confidentiality of Medical Information Act;
3) Sandra Lassiter's claim against LabCorp under the California Consumers Legal Remedies Act;
4) George Rothwell's claim against LabCorp under the Kentucky Consumer Protection Act;
5) David Finch's claim against LabCorp under the Kansas Consumer Protection Act;
6) Carol Kaplan's claim against LabCorp under the Maryland Consumer Protection Act;
7) Tatyana Shulman's claim against LabCorp under the Massachusetts Consumer Protection Act; and

Plaintiffs may amend the Complaint within 30 days of this Order to cure any deficiencies identified herein.

SO ORDERED.

/s Madeline Cox Arleo
MADELINE COX ARLEO
UNITED STATES DISTRICT JUDGE

[31] LabCorp also argues that MPIPA specifically permits it to disclose personal information to nonaffiliated third-party service providers like AMCA. Md. Code Ann. Com. Law § 14-3503(b). However, this permission does not absolve LabCorp of its general responsibility to "implement and maintain reasonable security procedures" which arguably prohibits negligence in disclosing that information. Id. 14-3503(a). As such, the Court will not dismiss the MPIPA claim for this reason.